Claims

1. A system for providing authentication of data communication over a communication link (104) between a client (100) and an agent (102) in accordance with an ordinarily insecure network communication protocol, the protocol comprising a communal string field for an appliance in the data communication, **characterized** in that, a string to be applied once, based on a shared seed between the client and the agent, is adapted to be incorporated into the communal string field to be transmitted between the client and the agent for authentication, wherein the string is determined by a substantially similar algorithm at both the client and the agent based on the shared seed.

2. A system according to claim 1, wherein a second string adapted to be applied once, based on the shared seed, is determined if either the client or the agent has applied the once applied string once.

3. A system according to claim 2, wherein the transmitted once applied string of a transmitting entity and the generated once applied string of a receiving network entity match for each string calculation round, and any other pair of the strings does not match, wherein the client and the agent comprise a transmitting network entity and a receiving network entity depending on an operational mode of the client and the agent in the communication link, wherein the roles can be changed.

4. A system according to claim 1, wherein the shared seed is based on a random number generator and is generated at either one of the client or the agent, and communicated to the one, which did not generate the shared seed.

5. A system according to any preceding claim, wherein the ordinarily insecure network communication protocol comprises Simple Network Management Protocol (SNMP).

6. A system according to any preceding claim, wherein the communication link (104) comprises Internet.

7. A system according to any preceding claim, wherein the algorithm generates a new string to be applied once, which string is based on the seed and on a secure random logic for being difficult to copy a pattern of a plurality of the strings.

8. A system according to claim 1, wherein the client and the agent remain synchronized in an operation loop of currently generated and once applied string by an acknowledgement message between the client and the agent.

9. A system according to claim 1, wherein the client or the agent sets an operation in accordance with the data communication unauthorized, if the string to be applied once, which is transmitted therebetween, does not correspond with a generated string to be applied once of a receiving network entity, wherein the client and the agent comprise a transmitting network entity and the receiving network entity depending on an operational mode of the client and the agent in the communication link, wherein the roles can be changed.

10. An apparatus (100,102) for providing authentication of data communication over a communication link (104) between a client (100,102) and an agent (100,102) in accordance with an ordinarily insecure network communication protocol, the protocol comprising a communal string field for an appliance in the data communication, **characterized** in that a string to be applied once, based on a shared seed between the client and the agent, is adapted to be incorporated into the communal string field to be transmitted between the client and the agent for authentication, wherein the once applied string is determined by a substantially similar algorithm at both the client and the agent based on the shared seed.

11. A method for authentication of data communication over a communication link (104) between a transmitting network entity (100,102) and a receiving network entity (100,102) in accordance with an ordinarily insecure network communication protocol, the protocol comprising a communal string field for an appliance in the data communication, **characterized** in that the method comprises the steps of:

establishing a seed at the either network entity for sharing the seed with the one network entity, which did not establish the seed,

sharing the seed with the one network entity, which did not establish the seed,

generating a string to be applied once based on the shared seed at both the transmitting network entity and the receiving network entity,

incorporating, at a transmitting network entity, the string into the communal string field for transmitting a message in accordance with the ordinarily insecure network communication protocol,

receiving the message at the receiving network entity,

checking the string of the communal string field of the message for correspondence with the string, which is calculated, at the receiving network entity, and

authenticating the message if there is a correspondence between the string of the communal string field of the message and the generated string.

12. A method according to claim 11, further comprising the steps of

generating a second string to be applied once based on the shared seed at both the transmitting network entity and the receiving network entity,

incorporating, at the transmitting network entity, the second string into the communal string field for transmitting a second message in accordance with the ordinarily insecure network communication protocol,

receiving the second message at the receiving network entity,

checking the second string of the communal string field of the second message for correspondence with the second string, which is calculated, at the receiving network entity, and

authenticating the second message if there is a correspondence between the second string of the communal string field of the second message and the generated second string.

13. A method according to claim 11, wherein the transmitting network entity and the receiving network entity comprise a client and an agent depending on an operational mode of the transmitting network entity and the receiving network entity in the communication link, wherein the roles can be changed.